The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

TLP: WHITE
Disclosure is not limited. Subject to standard copyright rules, TLP: WHITE information may be distributed without restriction.
http://www.us-cert.gov/tlp/

DATE(S) ISSUED:
04/20/2017

SUBJECT:
Multiple Vulnerabilities in VMware Products Could Allow for Code Execution

OVERVIEW:
Multiple vulnerabilities have been discovered in VMware Unified Access Gateway, VMware Horizon View, VMware Horizon View Client for Windows, and VMware Workstation Pro and Player. VMWare Unified Access Gateway is a virtual appliance primarily designed to allow secure remote access to VMware end-user computing resources from authorized users connecting from the Internet. VMware Horizon View and the Client allow a user to connect to their VMware Horizon virtual desktop from various devices. VMware Workstation Pro and VMware Workstation Player are applications that can allow for multiple operating systems as virtual machines on a single PC. Successful exploitation of the most severe of these vulnerabilities could allow for code execution in the context of the logged on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be less impacted than those who operate with administrative user rights.

THREAT INTELLIGENCE:
There have been no reports of these vulnerabilities being exploited in the wild.

SYSTEMS AFFECTED:
- VMware Unified Access Gateway 2.8.x versions prior to 2.81
- VMware Horizon View 7.x versions prior to 7.1.0
- VMware Horizon View Client for Windows 4.x versions prior to 4.4.0
- VMware Workstation Pro and Player 12.x versions prior to 12.5.3

RISK:
Government:
- Large and medium government entities: **High**
- Small government entities: **Medium**

Businesses:
- Large and medium business entities: **High**
- Small business entities: **Medium**

Home users: Low

TECHNICAL SUMMARY:
Multiple vulnerabilities have been discovered in VMware Unified Access Gateway, VMware Horizon View, VMware Horizon View Client for Windows, and VMware Workstation Pro and Player. The most severe of these vulnerabilities could allow for code execution. Details of these vulnerabilities are as follows:

- A heap-overflow vulnerability in Unified Access Gateway and Horizon View that allows a remote attacker to execute code on the security gateway (CVE-2017-4907).
- Two heap buffer-overflow vulnerabilities in VMware Workstation and Horizon View Client for Windows that may allow a guest to execute code or perform a denial of service attack (CVE-2017-4908, CVE-2017-4909).
- Three out-of-bounds read/write vulnerabilities in VMware Workstation and Horizon View Client for Windows that may allow a guest to execute code or perform a denial of service attack (CVE-2017-4910, CVE-2017-4911, CVE-2017-4912).
- An integer-overflow vulnerability in VMware Workstation and Horizon View Client for Windows that allows a guest to execute code or perform a denial of service attack (CVE-2017-4913).

Successful exploitation of the most severe of these vulnerabilities could allow for code execution in the context of the logged on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be less impacted than those who operate with administrative user rights.

RECOMMENDATIONS:
The following actions should be taken:

- Apply appropriate patches provided by VMware to vulnerable systems immediately after appropriate testing.
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.
- Apply the Principle of Least Privilege to all systems and services.

REFERENCES:
CVE:
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-4907
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-4908
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-4909
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-4910
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-4911
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-4912
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-4913

VMware
http://www.vmware.com/security/advisories/VMSA-2017-0008.html

http://www.us-cert.gov/tlp/